

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI**

ANGEL JOEL GUSMAN NEGRON, ALMA  
SUE CROFT, TIFFANY ROSE FARRAND,  
COURTNEY SUSANNE BROWN,  
VIKESHA ANDREALL EXFORD,  
CHERYL RENEE HAYES, LINDA SUE  
DUNN, CHRISTINA MARIE  
MCCLELLAN, LEAH SHATE WILLIS,  
JILL RADLEY, MATTIE RETHA  
BOYDEN, DONALD WAYNE PITCHERS  
JUNIOR, GEORGE GOUNARIS, and  
MICHAEL DARRYL CUNNINGHAM,  
individually and on behalf of all others  
similarly situated,

Plaintiffs,

v.

ASCENSION HEALTH, ASCENSION  
HEALTH ALLIANCE, ASCENSION  
HEALTH – IS INC. D/B/A ASCENSION  
TECHNOLOGIES,

Defendants.

Case No. 4:24-cv-00669-JAR

**AMENDED CLASS ACTION  
COMPLAINT**

JURY TRIAL DEMANDED

**CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Angel Joel Gusman Negrón, Alma Sue Croft, Tiffany Rose Farrand, Courtney Susanne Brown, Vikesha Andreall Exford, Cheryl Renee Hayes, Linda Sue Dunn, Christina Marie McClellan, Leah Shate Willis, Jill Radley, Mattie Retha Boyden, Donald Wayne Pitchers, Jr., George Gounaris, and Michael Darryl Cunningham (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this Amended Class Action Complaint against Ascension Health, Ascension Health Alliance, and Ascension Health – IS Inc. d/b/a Ascension Technologies (“Defendants” or “Ascension”), and allege, upon personal knowledge as to their own actions and their counsel’s investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. In or about May 2024, Defendants, a Catholic health-system that “includes approximately 134,000 associates, 35,000 affiliated providers and 140 hospitals, serving communities in 19 states and the District of Columbia,”<sup>1</sup> lost control over its computer network and the highly sensitive information of Plaintiffs and Class members, who are current and former patients of Defendants, in a data breach perpetrated by cybercriminals (the “Data Breach”). Based on Defendants’ public filings, the Breach affected at least hundreds of individuals.<sup>2</sup> However, Ascension has confirmed that its reported figure of 500 affected individuals was merely an interim figure, used as a placeholder until it determines the actual number of victims<sup>3</sup>—which is likely far higher.

2. According to Defendants’ Online Notice, on May 8, 2024, Defendants detected unusual activity in its system, which it later revealed was a ransomware attack.<sup>4</sup> Over a month later, Defendants confirmed that the hackers were able to take files from its servers, including files containing “Protected Health Information (PHI) and Personally Identifiable Information (PII).”<sup>5</sup> Nearly five months after Defendants discovered the attack, they have still not explained how long the hackers were in its systems, which not only strongly implies that it does not know, but also that Defendants’ logging, monitoring, and alerting systems were insufficient as compared to industry standards and were incapable of identifying malicious activity.

3. Likewise, as of October 7, 2024, Defendants have not provided notice of the Data

---

<sup>1</sup> <https://about.ascension.org/about-us>.

<sup>2</sup> U.S. Department of Health and Human Services Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information* (last accessed Oct. 2, 2024), [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf).

<sup>3</sup> Steve Alder, *Ascension Ransomware Attack Hurts Financial Recovery*, The HIPAA Journal (Sep. 20, 2024), <https://www.hipaajournal.com/ascension-cyberattack-2024>.

<sup>4</sup> <https://about.ascension.org/cybersecurity-event>.

<sup>5</sup> *Id.*

Breach to breach victims. Besides violating several breach notification laws, the failure to provide timely notice demonstrates that Defendants did not have adequate logging and monitoring to even understand the scope of the Data Breach.

4. On information and belief, the information compromised in the Data Breach encompasses both personally identifiable information (“PII”)<sup>6</sup> and personal health information (“PHI”)<sup>7</sup> (collectively, “Private Information”).

5. In or around May 9, 2024, Ascension posted a notice on its website, informing Plaintiffs and the Class Members that:

On Wednesday, May 8, we detected unusual activity on select technology network systems, which we now believe is due to a cybersecurity event. At this time we continue to investigate the situation. We responded immediately, initiated our investigation and activated our remediation efforts. Access to some systems have been interrupted as this process continues.

Our care teams are trained for these kinds of disruptions and have initiated procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible. There has been a disruption to clinical operations, and we continue to assess the impact and duration of the disruption.

We have engaged Mandiant, a third party expert, to assist in the investigation and remediation process, and we have notified the appropriate authorities. Together, we

---

<sup>6</sup> The Federal Trade Commission defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the Data Breach.

<sup>7</sup> Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d et seq., and its implementing regulations (“HIPAA”), “protected health information” is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. “Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP’T FOR HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last accessed Apr. 16, 2020). Ascension is clearly a “covered entity” and some of the data compromised in the Disclosure that this action arises out of is “protected health information,” subject to HIPAA.

are working to fully investigate what information, if any, may have been affected by the situation. Should we determine that any sensitive information was affected, we will notify and support those individuals in accordance with all relevant regulatory and legal guidelines.<sup>8</sup>

6. Defendants’ public Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its victims how many people were impacted, the identity of the cybercriminals who perpetrated this Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have never been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected. Instead, Ascension has simply been silent, posting its last update on June 14, 2024.<sup>9</sup>

7. Although Ascension downplays the incident with qualifiers like “potentially” and “may,” Defendants are aware that cybercriminals intentionally targeted them for the highly sensitive Private Information they store on their computer network, attacked and bypassed the insufficiently secured network, and exfiltrated the highly sensitive Private Information of victims. As a result, the Private Information of Plaintiffs and Class Members remain in the hands of those cyber-criminals.

8. Indeed, if Ascension had implemented and maintained reasonable, industry standard alerting systems like endpoint detection and response (“EDR”), extended detection and response (“XDR”), data loss prevention (“DLP”), and Security Information and Event Management (“SIEM”), Defendants likely would have recognized the malicious activity on its information systems in time to stop the attack before the hackers could steal Plaintiffs’ and the proposed Class Members’ highly sensitive Private Information.

---

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

9. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

10. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Private Information misuse.

11. The exposed Private Information of Plaintiffs and Class Members can—and likely will—be sold or traded on the dark web or other underground markets. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiffs and Class Members now face an imminent and lifetime risk of identity theft and fraud.

12. Additionally, because of Defendants' delayed response, Plaintiffs and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

13. Plaintiffs bring this action on behalf of all United States residents whose Private Information was compromised because of Defendants' failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware and software containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to violations of the common law and violates federal and state statutes.

14. Plaintiffs and Class Members have suffered injury because of Defendants' conduct. These injuries include: (i) damages for the unauthorized and unconsented use of their Private

Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) other consequential damages as a result of the violation of Defendants' duties to Plaintiffs and Class Members, and (iv) the continued and substantially increased risk to their Private Information which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

15. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

16. Plaintiff Angel Joel Gusman Negron is and at all relevant times was a citizen of the State of Illinois and the United States. Plaintiff is a resident of the State of Illinois and intends to remain domiciled in Illinois.

17. Plaintiff Alma Sue Croft is and at all relevant times was a citizen of the State of Alabama and the United States. Plaintiff is a resident of the State of Alabama and intends to remain domiciled in Alabama.

18. Plaintiff Tiffany Rose Farrand is and at all relevant times was a citizen of the State of Wisconsin and the United States. Plaintiff is a resident of the State of Wisconsin and intends to remain domiciled in Wisconsin.

19. Plaintiff Courtney Susanne Brown is and at all relevant times was a citizen of the State of Florida and the United States. Plaintiff is a resident of the State of Florida and intends to remain domiciled in Florida.

20. Plaintiff Vikesha Andreall Exford is and at all relevant times was a citizen of the State of Alabama and the United States. Plaintiff is a resident of the State of Alabama and intends to remain domiciled in Alabama.

21. Plaintiff Cheryl Renee Hayes is and at all relevant times was a citizen of the State of Oklahoma and the United States. Plaintiff is a resident of the State of Oklahoma and intends to remain domiciled in Oklahoma.

22. Plaintiff Linda Sue Dunn is and at all relevant times was a citizen of the State of Arkansas and the United States. Plaintiff is a resident of the State of Arkansas and intends to remain domiciled in Arkansas.

23. Plaintiff Christina Marie McClellan is and at all relevant times was a citizen of the State of Texas and the United States. Plaintiff is a resident of the State of Texas and intends to remain domiciled in Texas.

24. Plaintiff Leah Shate Willis is and at all relevant times was a citizen of the State of Michigan and the United States. Plaintiff is a resident of the State of Michigan and intends to remain domiciled in Michigan.

25. Plaintiff Jill Radley is and at all relevant times was a citizen of the State of Wisconsin and the United States. Plaintiff is a resident of the State of Wisconsin and intends to remain domiciled in Wisconsin.

26. Plaintiff Mattie Retha Boyden is and at all relevant times was a citizen of the State of Illinois and the United States. Plaintiff is a resident of the State of Illinois and intends to remain domiciled in Illinois.

27. Plaintiff Donald Wayne Pitchers Junior is and at all relevant times was a citizen of the State of Indiana and the United States. Plaintiff is a resident of the State of Indiana and intends to remain domiciled in Indiana.

28. Plaintiff George Gounaris is and at all relevant times was a citizen of the State of Indiana and the United States. Plaintiff is a resident of the State of Indiana and intends to remain domiciled in Indiana.

29. Plaintiff Michael Darryl Cunningham is and at all relevant times was a citizen of the State of Kentucky and the United States. Plaintiff is a resident of the State of Kentucky and intends to remain domiciled in Kentucky.

30. Defendant Ascension Health is a nonprofit corporation organized under the state laws of Missouri with its principal place of business located at 4600 Edmundson Rd St. Louis, MO 63134. Ascension Health is “a part of the Ascension catholic health ministry.” “Ascension Health provides a variety of noncash centralized system office support in furtherance of the mission of

the Ascension sponsor and the other supported organizations listed in Part I.”<sup>10</sup> Ascension Health is a subsidiary of Ascension Health Alliance.<sup>11</sup>

31. Defendant Ascension Health Alliance is a nonprofit corporation organized under the state laws of Missouri with its principal place of business located at 4600 Edmundson Rd St. Louis, MO 63134. Ascension Health Alliance is the parent of both Ascension Health – IS Inc. and Ascension Health.<sup>12</sup>

32. Ascension Health – IS Inc. d/b/a Ascension Technologies is a nonprofit corporation organized under the laws of Missouri with its principal place of business located at 4600 Edmundson Rd St. Louis, MO 63134. Ascension Health – IS Inc., “was formed to provide information technology (‘i.t.’) and application support services to the member entities of Ascension Health Alliance. ... in addition to providing i.t. and application support services, AHIS provides an array of services including strategic leadership, development of strategies around i.t. investments, consolidation of i.t. contracts, and efficient and cost-effective installation and support for system i.t. investments. Ascension Health Alliance, a tax-exempt, catholic health care organization, is the parent of this organization...”<sup>13</sup>

### III. JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members exceeds 499, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

---

<sup>10</sup> <https://projects.propublica.org/nonprofits/organizations/311662309/202401369349308790/full>

<sup>11</sup> <https://about.ascension.org/-/media/project/ascension/about/section-about/financials/2023/consolidated-ascension-financial-statements-q4-fy23.pdf> at p.12.

<sup>12</sup> *Id.*

<sup>13</sup> <https://projects.propublica.org/nonprofits/organizations/651257719/202441369349310089/full>

34. This Court has personal jurisdiction over Defendants because they operate and are headquartered in this District and conduct substantial business in this District.

35. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendants are based in this District, maintain Plaintiffs' and Class Members' Private Information in this District, and have caused harm to Plaintiffs and Class Members in this District.

#### IV. FACTUAL ALLEGATIONS

##### *Defendants Ascension Health*

36. Ascension touts itself as “one of the nation’s leading non-profit and Catholic health systems,” which is “positioned to meet the evolving needs of the people and communities we serve in the rapidly changing healthcare environment” with an “800-year legacy” of providing healthcare.<sup>14</sup>

37. In its Notices of Privacy Practices, Ascension acknowledges that its patients have specific privacy rights that protect the confidentiality of their health information.<sup>15</sup>

38. Among other things, Ascension recognizes that it is required to:

- a. “Maintain the privacy and security of your health information,”; and
- b. “Notify you if a breach occurs that may have compromised the privacy or security of your identifiable health information.”<sup>16</sup>

39. As a healthcare company that handles highly sensitive and personal information, Ascension understood the need to protect its patients' Private Information and prioritize its data security.

---

<sup>14</sup> <https://about.ascension.org/about-us/history-sponsorship>.

<sup>15</sup> See e.g., Ascension St. Vincent's Joint Notice of Privacy Practices, [https://healthcare.ascension.org/-/media/healthcare/npp/alabama/al\\_ascension-st-vincent's\\_english.pdf](https://healthcare.ascension.org/-/media/healthcare/npp/alabama/al_ascension-st-vincent's_english.pdf) (last accessed Oct. 2, 2024).

<sup>16</sup> *Id.*

40. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, and to make only authorized disclosures of this information.

41. Despite recognizing its duty to do so, on information and belief, Ascension has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Ascension leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Private Information.

***Defendants' Data Breach***

42. Plaintiffs are former and current patients of Ascension. As a condition of receiving healthcare services from Ascension, Plaintiffs were required to provide Ascension with their Private Information and in return, reasonably expected that Ascension will safeguard that highly sensitive and confidential information. Upon information and belief, the Private Information entrusted to Ascension by Plaintiffs and the Class included: full names, dates of birth, Social Security numbers, health plan information, medical information, and financial information.

43. On information and belief, after collecting its patients' Private Information, Ascension maintains it in its computer systems unencrypted and without adequate security controls in place to identify potential unauthorized access.

44. Ascension also creates and stores medical records and other PHI for its patients, including records of treatments and diagnoses, lab results, and prescription information.

45. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Ascension explicitly and implicitly agrees to safeguard the data using reasonable means according to its internal policies and federal law. As such, Ascension knew

or should have known that it was responsible to protect Plaintiffs’ and Class Members’ Private Information from unauthorized disclosure.

46. Ascension failed in its duties on or before May 8, 2024, when its inadequate security practices resulted in the Data Breach and allowed cybercriminals to remove files from its servers.<sup>17</sup> Ascension admits in its online notice that it believes the files removed by the cybercriminals included “Protected Health Information (PHI) and Personally Identifiable Information (PII).”<sup>18</sup>

47. In other words, Ascension’s investigation revealed that its network had been hacked by cybercriminals and that Ascension’s inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain and steal files containing a treasure trove of Ascension’s patients’ Private Information — the scope of which Ascension is still unable to determine and disclose to Plaintiffs and Class Members.

48. Despite its duties and alleged commitments to safeguard Private Information, Ascension does not follow industry standard practices in securing patients’ Private Information, as evidenced by the Data Breach.

49. Cybercriminals need not harvest a person’s Social Security number or financial account information to commit identity fraud or misuse Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create “Fullz” packages —or elements of stolen personal information bundled together—which can then be used to commit identity theft or fraud.

50. Moreover, the compromise of Plaintiffs’ and Class Members’ PHI immediately exposes victims to specific types of health care fraud, including fraudsters securing medical

---

<sup>17</sup> <https://about.ascension.org/cybersecurity-event>.

<sup>18</sup> *Id.*

treatment, elective surgeries, and filled prescriptions in the victims' names. According to Allstate, "medical identity theft has an annual economic impact of around \$41 billion a year."<sup>19</sup>

51. Ascension breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Ascension's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches;
- b. Failing to adequately protect patients Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions, including through the use of EDR, XDR, DLP, and SIEM tools;
- d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Ascension's networks, and to maintain adequate email security practices;
- e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;
- f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- g. Failing to comply with HIPAA; and
- h. Failing to adhere to industry standards for cybersecurity.

---

<sup>19</sup> Allstate Identity Protection, *Why is the Healthcare Industry the Biggest Victim of Identity Theft and Data Breaches?*, BUSINESS INSIGHT, <https://www.allstateidentityprotection.com/business/content-hub/why-healthcare-industry-biggest-victim-of-identity-theft-and-data-breaches>.

52. Potentially as the result of outdated antivirus and malware protection software, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendants' IT systems and remove data which contained unsecured and unencrypted Private Information.

53. As a result of the Data Breach, Plaintiffs and Class Members have suffered injuries and now face an imminent and continued risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants and suffered other consequential losses because of the Data Breach.

54. Through its Online Notice of Data Security Incident on its website, Ascension recognized the actual imminent harm and injury that flowed from the Data Breach by offering victims credit monitoring services and identity theft protection services and "encourage[ing] all Ascension patients and staff who are concerned to take advantage of these services."<sup>20</sup> The monitoring offered by Ascension is incomplete and inadequate to address Plaintiffs' and Class Members' harm as a result of the Data Breach.

55. Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches.

56. To date, Defendants have done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered because of the Data Breach. Defendants have merely offered Plaintiffs and Class Members inadequate credit monitoring. But this does not compensate

---

<sup>20</sup> <https://about.ascension.org/cybersecurity-event>.

them for damages incurred and time spent dealing with the Data Breach, the lost value of their Personal Information, or the consequential damages necessary to put Plaintiffs and Class Members in the position they would have been in but for the Data Breach.

***The Data Breach Was a Foreseeable Risk of which Ascension Was on Notice.***

57. Plaintiffs and Class Members value their Private Information, as in today's electronic-centric world, their Private Information is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

58. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>21</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>22</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>23</sup> This damage is equivalent to the repeated sale of a non-exclusive license to Plaintiffs' and Class Members' Personal Information.

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

60. This data demands a much higher price on the black market. Martin Walter, senior

---

<sup>21</sup> Anita George, *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs*, DIGITAL TRENDS (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs>.

<sup>22</sup> Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web>.

<sup>23</sup> *For Sale in the Dark*, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark> (last accessed Sept. 13, 2024).

director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information...[is] worth more than 10x on the black market.”<sup>24</sup>

61. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

62. Individuals, like Plaintiffs and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person’s identity and is likened to accessing your DNA for hacker’s purposes.

63. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

64. The Social Security Administration has warned that “a new number probably won’t solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won’t guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same.”<sup>25</sup>

65. Ascension’s data security obligations were also particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

---

<sup>24</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10X Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

<sup>25</sup> Social Security Admin., *Identity Theft and Your Social Security Number*, Pub. No. 05-10064 (July 2021), <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

66. According to Advent Health University, when an electronic health record “lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to \$1,000.”<sup>26</sup>

67. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

68. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their “highly prized” medical records. “[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS’ Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents.”<sup>27</sup>

69. According to the U.S. Department of Health and Human Services, “Ransomware and hacking are the primary cyber-threats in health care.” Ransomware cyberattacks reported to the U.S. Dept. of Health and Human Services, Office for Civil Rights have increased 278% from 2018-2023.<sup>28</sup>

70. A study of ransomware cyberattacks from 2016-2023 on healthcare organizations in the U.S. found: 539 individual ransomware attacks on healthcare organizations; 9,780 healthcare organizations affected; Approximately 52.3 million individual patient records impacted;

---

<sup>26</sup> Advent Health Univ., *5 Important Elements to Establish Data Security in Healthcare* (May 21, 2020), <https://www.ahu.edu/blog/data-security-in-healthcare>.

<sup>27</sup> Steve Adler, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), <https://www.hipaajournal.com/why-do-criminals-target-medical-records>.

<sup>28</sup> U.S. Department of Health and Human Services, *HHS’ Office for Civil Rights Settles Ransomware Cyber-Attack Investigation*, (Oct. 31, 2023), <https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html>.

Ransomware demands varying from \$1,600 to \$10 million; Average downtime across all years of 14 days, with a total of 6,347 days of downtime; Hackers receiving payment in 31 out of 160 cases where the healthcare organization “disclosed whether or not they paid the ransom”; and Overall cost of the attacks of approximately \$77.5 billion in downtime alone.<sup>29</sup>

71. In 2023 alone, 46 hospital systems suffered ransomware attacks in 2023, which affected 141 hospitals directly affected, wherein patient care was disrupted “due to the lack of access to IT systems and patient data.”<sup>30</sup>

72. Healthcare organizations are easy targets because “even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized.”<sup>31</sup>

73. The HIPAA Journal article goes on to explain that patient records, like those stolen from Ascension, are “often processed and packaged with other illegally obtained data to create full record sets (the previously mentioned Fullz package) that contain extensive information on individuals, often in intimate detail.” The record sets are then sold on dark web sites to other criminals and “allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities.”<sup>32</sup>

---

<sup>29</sup> Paul Bischoff, *Ransomware Attacks on Healthcare Organizations Have Cost the US Economy \$77.5bn in Downtime Alone*, Comparitech, (Oct. 23, 2023), <https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data>.

<sup>30</sup> Steve Adler, *At Least 141 Hospitals Directly Affected by Ransomware Attacks in 2023*, THE HIPAA JOURNAL, (JAN. 4, 2024) <https://www.hipaajournal.com/2023-healthcare-ransomware-attacks>.

<sup>31</sup> Steve Adler, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), <https://www.hipaajournal.com/why-do-criminals-target-medical-records>.

<sup>32</sup> *Id.*

74. Data breaches such as the one experienced by Defendants have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

75. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.<sup>33</sup>

76. These significant increases in attacks to companies, particularly those in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Ascension.

77. A study by Experian found that the average total cost of medical identity theft is “nearly \$13,500” per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.<sup>34</sup> Victims of healthcare data breaches often find themselves “being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores.”<sup>35</sup>

78. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

---

<sup>33</sup> Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

<sup>34</sup> Brian O’Connor, *Health Care Data Breach: What to Know About Them and What to Do After One*, EXPERIAN (Mar. 31, 2023), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one>.

<sup>35</sup> *Id.*

continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

79. It is incorrect to assume that reimbursing a victim for a financial loss due to fraud makes that individual whole again. Like the GAO's study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."<sup>36</sup> In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."<sup>37</sup>

80. As the fraudulent activity resulting from the Data Breach may not come to light for years, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

***Defendants Failed to Comply with FTC Guidelines.***

81. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

82. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

---

<sup>36</sup> Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEP'T OF JUSTICE (Sept. 2015), <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf> (revised Nov. 13, 2017).

<sup>37</sup> *Id.*

understand their network's vulnerabilities; and implement policies to correct any security problems.<sup>38</sup>

83. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

84. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

86. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

<sup>38</sup> Federal Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

***Defendants Failed to Comply with Industry Standards.***

87. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

88. To prevent and detect unauthorized cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with at least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>39</sup>

89. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want

---

<sup>39</sup> *Id.* at 3–4.

to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....<sup>40</sup>

90. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure Internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs

---

<sup>40</sup> Cybersecurity and Infrastructure Security Agency, *Protecting Against Ransomware* (April 11, 2019), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (revised Sept. 2, 2021).

- Analyze logon events

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>41</sup>

91. Defendant Ascension made the choice to collect and store the Private Information of Plaintiffs and Class Members, and therefore could and should have implemented all the above measures to prevent and detect cyberattacks.

92. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

***Defendants Failed to Comply with HIPAA.***

94. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

---

<sup>41</sup> Microsoft Threat Intelligence, *Human-Operated Ransomware Attacks: A Preventable Disaster*, (Mar. 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster>.

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.<sup>42</sup>

95. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained.<sup>43</sup>

96. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards by

---

<sup>42</sup> HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

<sup>43</sup> See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

Ascension's workforce in violation of 45 C.F.R. § 164.306(a)(4);

- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

97. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrated Defendants failed to comply with safeguards mandated by HIPAA regulations.

### ***Plaintiffs' Experiences***

#### **Plaintiff Alma Sue Croft**

98. Plaintiff Alma Sue Croft is and at all relevant times was a citizen of the State of Alabama and the United States.

99. Plaintiff Croft was an Ascension patient at the time of the Data Breach.

100. In the course of obtaining treatment, Plaintiff Croft was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Croft reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

101. In the course of obtaining treatment, Plaintiff Croft received a copy of Ascension's Notice of Privacy Practices.

102. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

103. As a result of the Data Breach, Plaintiff Croft has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Croft has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Croft has already been notified by her credit monitoring service that her PII and PHI has been disseminated on the Dark Web.

104. To date, Plaintiff Croft has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Croft values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

105. Had Plaintiff Croft been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Croft has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Croft anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

106. Plaintiff Croft suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

107. The Data Breach has caused Plaintiff Croft to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

108. As a result of the Data Breach, Plaintiff Croft is and will continue to be at increased risk of identity theft and fraud for years to come.

109. Plaintiff Croft has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

110. Upon information and belief, Ascension continues to store and/or share Plaintiff Croft's PII and PHI on its internal systems. Thus, Plaintiff Croft has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Angel Joel Gusman Negrón

111. Plaintiff Angel Joel Gusman Negrón is and at all relevant times was a citizen of the State of Illinois and the United States.

112. Plaintiff Negrón was an Ascension patient at the time of the data breach.

113. In the course of obtaining treatment, Plaintiff Negrón was required, directly or indirectly, to provide his PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with his PII and PHI, Plaintiff Negrón reasonably expected that his PII and PHI would remain safe and not be accessed by unauthorized third parties.

114. In the course of obtaining treatment, Plaintiff Negrón received a copy of Ascension's Notice of Privacy Practices.

115. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's PII and PHI in its system.

116. As a result of the Data Breach, Plaintiff Negrón has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to:

researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Negrón has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

117. To date, Plaintiff Negrón has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Negrón values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

118. Had Plaintiff Negrón been informed of Ascension's insufficient data security measures to protect his PII and PHI, he would not have willingly provided his PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Negrón has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Negrón anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

119. Plaintiff Negrón suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) damages for unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

120. The Data Breach has caused Plaintiff Negron to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

121. As a result of the Data Breach, Plaintiff Negron is and will continue to be at increased risk of identity theft and fraud for years to come.

122. Plaintiff Negron has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

123. Upon information and belief, Ascension continues to store and/or share Plaintiff Negron's PII and PHI on its internal systems. Thus, Plaintiff Negron has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Vikesha Andreall Exford

124. Plaintiff Vikesha Andreall Exford is and at all relevant times was a citizen of the State of Alabama and the United States.

125. Plaintiff Exford was an Ascension patient at the time of the data breach.

126. In the course of obtaining treatment, Plaintiff Exford was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Exford reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

127. In the course of obtaining treatment, Plaintiff Exford received a copy of Ascension's Notice of Privacy Practices.

128. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

129. As a result of the Data Breach, Plaintiff Exford has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Exford has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

130. Since the Data Breach, Plaintiff Exford has had fraudulent charges on her bank account, requiring her to lock and then get a new debit card. While her debit card was locked, Plaintiff Exford temporarily lost insurance coverage for her vehicle as the charge was bounced due to the lock. This required Plaintiff Exford to pay a \$45 reinstatement fee and a \$25 late fee, both of which remain unreimbursed. Plaintiff Exford has also received an alert from her credit

monitoring service that her email address and Social Security number were compromised. Plaintiff Exford has also seen an increase in spam texts, emails, and phone calls since the breach.

131. To date, Plaintiff Exford has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Exford values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

132. Had Plaintiff Exford been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Exford has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Exford anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

133. Plaintiff Exford suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

134. The Data Breach has caused Plaintiff Exford to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

135. As a result of the Data Breach, Plaintiff Exford is and will continue to be at increased risk of identity theft and fraud for years to come.

136. Plaintiff Exford has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

137. Upon information and belief, Ascension continues to store and/or share Plaintiff Exford's PII and PHI on its internal systems. Thus, Plaintiff Exford has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Linda Sue Dunn

138. Plaintiff Linda Sue Dunn is and at all relevant times was a citizen of the State of Arkansas and the United States.

139. Plaintiff Dunn was a former Ascension patient at the time of the data breach who received treatment in Florida.

140. In the course of obtaining treatment, Plaintiff Dunn was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Dunn reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

141. In the course of obtaining treatment, Plaintiff Dunn received a copy of Ascension's Notice of Privacy Practices.

142. Upon information and belief, at the time of the Data Breach, Ascension retained Plaintiff's PII and PHI in its system.

143. As a result of the Data Breach, Plaintiff Dunn has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Dunn has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Subsequent to the Data Breach, Plaintiff Dunn received notice that her PII or PHI is on the Dark Web.

144. To date, Plaintiff Dunn has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Dunn values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

145. Had Plaintiff Dunn been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Dunn has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Dunn

anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

146. Plaintiff Dunn suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

147. The Data Breach has caused Plaintiff Dunn to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff Dunn is and will continue to be at increased risk of identity theft and fraud for years to come.

149. Plaintiff Dunn has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

150. Upon information and belief, Ascension continues to store and/or share Plaintiff Dunn's PII and PHI on its internal systems. Thus, Plaintiff Dunn has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Courtney Susanne Brown

151. Plaintiff Courtney Susanne Brown is and at all relevant times was a citizen of the State of Florida and the United States.

152. Plaintiff Brown was an Ascension patient at the time of the Data Breach.

153. In the course of obtaining treatment, Plaintiff Brown was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Brown reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

154. In the course of obtaining treatment, Plaintiff Brown received a copy of Ascension's Notice of Privacy Practices.

155. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

156. As a result of the Data Breach, Plaintiff Brown has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Brown has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not

limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Brown has had unrelated and unrecognized things appear on her credit report since the Data Breach.

157. To date, Plaintiff Brown has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Brown values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

158. Had Plaintiff Brown been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Brown has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Brown anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

159. Plaintiff Brown suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and

available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

160. The Data Breach has caused Plaintiff Brown to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

161. As a result of the Data Breach, Plaintiff Brown is and will continue to be at increased risk of identity theft and fraud for years to come.

162. As a result of the Data Breach, Plaintiff Brown's medical care was impacted. Plaintiff Brown was at an Ascension facility on May 8, 2024 during the breach but despite being told she required urgent surgery, no surgery was performed due to Ascension's Data Breach.

163. Plaintiff Brown has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

164. Upon information and belief, Ascension continues to store and/or share Plaintiff Brown's PII and PHI on its internal systems. Thus, Plaintiff Brown has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Mattie Retha Boyden

165. Plaintiff Mattie Retha Boyden is and at all relevant times was a citizen of the State of Illinois and the United States.

166. Plaintiff Boyden was an Ascension patient at the time of the data breach.

167. In the course of obtaining treatment, Plaintiff Boyden was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and

address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Boyden reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

168. In the course of obtaining treatment, Plaintiff Boyden received a copy of Ascension's Notice of Privacy Practices.

169. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

170. As a result of the Data Breach, Plaintiff Boyden has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Boyden has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

171. Since the Data Breach Plaintiff Boyden has received a notification that her PII or PHI is on the Dark Web. Plaintiff Boyden has also seen an increase in spam texts, emails, and phone calls since the breach.

172. To date, Plaintiff Boyden has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Boyden values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

173. Had Plaintiff Boyden been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Boyden has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Boyden anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

174. Plaintiff Boyden suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

175. The Data Breach has caused Plaintiff Boyden to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

176. As a result of the Data Breach, Plaintiff Boyden is and will continue to be at increased risk of identity theft and fraud for years to come.

177. Plaintiff Boyden has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

178. Upon information and belief, Ascension continues to store and/or share Plaintiff Boyden's PII and PHI on its internal systems. Thus, Plaintiff Boyden has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Michael Darryl Cunningham

179. Plaintiff Michael Darryl Cunningham is and at all relevant times was a citizen of the State of Kentucky and the United States.

180. Plaintiff Cunningham was an Ascension patient at the time of the data breach.

181. In the course of obtaining treatment, Plaintiff Cunningham was required, directly or indirectly, to provide his PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with his PII and PHI, Plaintiff Cunningham reasonably expected that his PII and PHI would remain safe and not be accessed by unauthorized third parties.

182. In the course of obtaining treatment, Plaintiff Cunningham received a copy of Ascension's Notice of Privacy Practices.

183. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

184. As a result of the Data Breach, Plaintiff Cunningham has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to:

researching and verifying the legitimacy of the Data Breach; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Cunningham has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

185. Since the Data Breach Plaintiff Cunningham has received notification that his PII or PHI is on the Dark Web. Additionally, Plaintiff Cunningham, has had fraudulent activity on various accounts. Plaintiff Cunningham has also seen an increase in spam texts, emails, and phone calls since the breach.

186. To date, Plaintiff Cunningham has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Cunningham values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

187. As a result of the Data Breach, Plaintiff Cunningham was forced to reschedule and alter a medical procedure. Requiring him to have the procedure done at a different hospital.

188. Had Plaintiff Cunningham been informed of Ascension's insufficient data security measures to protect his PII and PHI, he would not have willingly provided his PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Cunningham has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Cunningham anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

189. Plaintiff Cunningham suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

190. The Data Breach has caused Plaintiff Cunningham to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

191. As a result of the Data Breach, Plaintiff Cunningham is and will continue to be at increased risk of identity theft and fraud for years to come.

192. Plaintiff Cunningham has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

193. Upon information and belief, Ascension continues to store and/or share Plaintiff Cunningham's PII and PHI on its internal systems. Thus, Plaintiff Cunningham has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Leah Shate Willis

194. Plaintiff Leah Shate Willis is and at all relevant times was a citizen of the State of Michigan and the United States.

195. Plaintiff Willis was an Ascension patient at the time of the data breach.

196. In the course of obtaining treatment, Plaintiff Willis was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Willis reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

197. In the course of obtaining treatment, Plaintiff Willis received a copy of Ascension's Notice of Privacy Practices.

198. Upon information and belief, at the time of the Data Breach, Ascension retained Plaintiff's PII and PHI in its system.

199. As a result of the Data Breach, Plaintiff Willis has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Willis has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Willis has also seen an increase in spam texts, emails, and phone calls since the breach.

200. As a result of the Data Breach, Plaintiff Willis' surgery to resolve a serious health issue was canceled leaving her in pain until the surgery could be rescheduled. Plaintiff Willis was able to get the surgery partially rescheduled but to date has not had the issue completely resolved.

201. Plaintiff Willis has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Willis values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

202. Had Plaintiff Willis been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Willis has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Willis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

203. Plaintiff Willis suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

204. The Data Breach has caused Plaintiff Willis to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

205. As a result of the Data Breach, Plaintiff Willis is and will continue to be at increased risk of identity theft and fraud for years to come.

206. Plaintiff Willis has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

207. Upon information and belief, Ascension continues to store and/or share Plaintiff Willis' PII and PHI on its internal systems. Thus, Plaintiff Willis has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Cheryl Renee Hayes

208. Plaintiff Cheryl Renee Hayes is and at all relevant times was a citizen of the State of Oklahoma and the United States.

209. Plaintiff Hayes was an Ascension patient at the time of the data breach.

210. In the course of obtaining treatment, Plaintiff Hayes was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Hayes reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

211. In the course of obtaining treatment, Plaintiff Hayes received a copy of Ascension's Notice of Privacy Practices.

212. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

213. As a result of the Data Breach, Plaintiff Hayes has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Hayes has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

214. After the Data Breach, Plaintiff Hayes has received notice that her PII and/or PHI are on the Dark Web. Plaintiff Hayes has also seen an increase in spam texts, emails, and phone calls since the breach.

215. To date, Plaintiff Hayes has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Hayes values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

216. Had Plaintiff Hayes been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Hayes has already suffered injury and remains at a

substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Hayes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

217. Plaintiff Hayes suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

218. The Data Breach has caused Plaintiff Hayes to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

219. As a result of the Data Breach, Plaintiff Hayes is and will continue to be at increased risk of identity theft and fraud for years to come.

220. As a result of the Data Breach, Plaintiff Hayes's medical care was compromised, she was delayed in refilling certain prescriptions and the pharmacy was unsure exactly what the

prescriptions were for since they were handwritten. Introducing additional stress to an already stressful situation.

221. Plaintiff Hayes has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

222. Upon information and belief, Ascension continues to store and/or share Plaintiff Hayes' PII and PHI on its internal systems. Thus, Plaintiff Hayes has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Christina Marie McClellan

223. Plaintiff Christina Marie McClellan is and at all relevant times was a citizen of the State of Texas and the United States.

224. Plaintiff McClellan was a former Ascension patient at the time of the data breach.

225. Plaintiff McClellan was last a patient of Ascension in 2023. In the course of obtaining treatment, Plaintiff McClellan was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff McClellan reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

226. In the course of obtaining treatment, Plaintiff McClellan received a copy of Ascension's Notice of Privacy Practices.

227. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

228. As a result of the Data Breach, Plaintiff McClellan has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to:

researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff McClellan has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

229. Plaintiff McClellan has seen an increase in spam texts, emails, and phone calls since the breach. These spam text messages have been personalized to her.

230. To date, Plaintiff McClellan has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff McClellan values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

231. Had Plaintiff McClellan been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff McClellan has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff McClellan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

232. Plaintiff McClellan suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the

Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

233. The Data Breach has caused Plaintiff McClellan to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

234. As a result of the Data Breach, Plaintiff McClellan is and will continue to be at increased risk of identity theft and fraud for years to come.

235. Plaintiff McClellan has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

236. Upon information and belief, Ascension continues to store and/or share Plaintiff McClellan's PII and PHI on its internal systems. Thus, Plaintiff McClellan has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Donald Wayne Pitchers Jr.

237. Plaintiff Donald Wayne Pitchers Jr. is and at all relevant times was a citizen of the State of Indiana and the United States.

238. Plaintiff Pitchers was an Ascension patient at the time of the data breach.

239. In the course of obtaining treatment, Plaintiff Pitchers was required, directly or indirectly, to provide his PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with his PII and PHI, Plaintiff Pitchers reasonably expected that his PII and PHI would remain safe and not be accessed by unauthorized third parties.

240. In the course of obtaining treatment, Plaintiff Pitchers received a copy of Ascension's Notice of Privacy Practices.

241. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

242. As a result of the Data Breach, Plaintiff Pitchers has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Pitchers has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

243. As a result of the Data Breach, Plaintiff Pitchers was unable to obtain necessary medical care. Despite having diabetes, Plaintiff Pitchers was not able to obtain his insulin on time and was forced to take a lower dose than prescribed to stretch out his medicine until he was able to get his prescription refilled.

244. Since the breach, Plaintiff Pitchers has been informed that his PII and PHI has appeared on the Dark Web.

245. To date, Plaintiff Pitchers has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Pitchers values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

246. Had Plaintiff Pitchers been informed of Ascension's insufficient data security measures to protect his PII and PHI, he would not have willingly provided his PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Pitchers has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Pitchers anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

247. Plaintiff Pitchers suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

248. The Data Breach has caused Plaintiff Pitchers to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed him of key details about the Data Breach's occurrence.

249. As a result of the Data Breach, Plaintiff Pitchers is and will continue to be at increased risk of identity theft and fraud for years to come.

250. Plaintiff Pitchers has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

251. Upon information and belief, Ascension continues to store and/or share Plaintiff Pitchers' PII and PHI on its internal systems. Thus, Plaintiff Pitchers has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff George Gounaris

252. Plaintiff George Gounaris is and at all relevant times was a citizen of the State of Indiana and the United States.

253. Plaintiff Gounaris was an Ascension patient and customer at the time of the data breach.

254. In the course of obtaining treatment and insurance, Plaintiff Gounaris was required, directly or indirectly, to provide his PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with his PII and PHI, Plaintiff Gounaris reasonably expected that his PII and PHI would remain safe and not be accessed by unauthorized third parties.

255. In the course of obtaining treatment, Plaintiff Gounaris received a copy of Ascension's Notice of Privacy Practices.

256. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

257. As a result of the Data Breach, Plaintiff Gounaris has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Gounaris has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Subsequent to the Data Breach Plaintiff Gounaris was notified that his PII or PHI was found on the Dark Web.

258. To date, Plaintiff Gounaris has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Gounaris values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

259. Had Plaintiff Gounaris been informed of Ascension's insufficient data security measures to protect his PII and PHI, he would not have willingly provided his PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Gounaris has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Gounaris

anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

260. Plaintiff Gounaris suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

261. The Data Breach has caused Plaintiff Gounaris to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed him of key details about the Data Breach's occurrence.

262. As a result of the Data Breach, Plaintiff Gounaris is and will continue to be at increased risk of identity theft and fraud for years to come.

263. Plaintiff Gounaris has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

264. Upon information and belief, Ascension continues to store and/or share Plaintiff Gounaris' PII and PHI on its internal systems. Thus, Plaintiff Gounaris has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

Plaintiff Jill Radley

265. Plaintiff Jill Radley is and at all relevant times was a citizen of the State of Wisconsin and the United States.

266. Plaintiff Radley was an Ascension patient at the time of the data breach.

267. In the course of obtaining treatment, Plaintiff Radley was required, directly or indirectly, to provide her PII and PHI, including name, Social Security number, date of birth, and address. When providing and entrusting Ascension with her PII and PHI, Plaintiff Radley reasonably expected that her PII and PHI would remain safe and not be accessed by unauthorized third parties.

268. In the course of obtaining treatment, Plaintiff Radley received a copy of Ascension's Notice of Privacy Practices.

269. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII and PHI in its system.

270. As a result of the Data Breach, Plaintiff Radley has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis; reviewing and remaining vigilant against medical fraud. Plaintiff Radley has spent significant time dealing with the Data

Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

271. Plaintiff Radley's bank account was compromised in August 2024. Because of this compromise and the large withdrawals, Plaintiff Radley was required to pay overdraft fees that have not been reimbursed. Plaintiff Radley has also seen an increase in spam texts, emails, and phone calls since the breach that are specifically targeted at her and include personal information related to her health issues.

272. To date, Plaintiff Radley has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Radley values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

273. Had Plaintiff Radley been informed of Ascension's insufficient data security measures to protect her PII and PHI, she would not have willingly provided her PII and PHI to Ascension. Given the highly sensitive nature of the PII and PHI stolen, and its likely subsequent dissemination to unauthorized parties, Plaintiff Radley has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Radley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

274. Plaintiff Radley suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) damages for the unauthorized disclosure of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the PII and PHI.

275. The Data Breach has caused Plaintiff Radley to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

276. As a result of the Data Breach, Plaintiff Radley is and will continue to be at increased risk of identity theft and fraud for years to come.

277. Plaintiff Radley has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Ascension's possession, is protected and safeguarded from future breaches.

278. Upon information and belief, Ascension continues to store and/or share Plaintiff Radley's PII and PHI on its internal systems. Thus, Plaintiff Radley has a continuing interest in ensuring that the PII and PHI is protected and safeguarded from future breaches.

## **V. CLASS ALLEGATIONS**

279. Plaintiffs bring this class action on behalf of themselves and on behalf of others similarly situated pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

280. The Class that Plaintiffs seek to represent is defined as follows:

All United States residents whose Personal Information was compromised in the Data Breach discovered by Ascension in May 2024, including all those individuals who receive notice of the breach.

281. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have controlling interests; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

282. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

283. Numerosity: The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach.

284. Commonality: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;
- b. Whether Defendants had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendants had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendants failed to adequately safeguard the Private Information

of Plaintiffs and Class Members;

- e. Whether and when Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;
- k. Whether Defendants violated the consumer protection statutes invoked herein;
- l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;
- m. Whether Defendants knowingly made false representations as to its data security practices;
- n. Whether Plaintiffs and Class Members are entitled to restitution because of Defendants' wrongful conduct; and

- o. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

285. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised because of the Data Breach, due to Defendants' misfeasance.

286. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Ascension has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

287. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

288. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will

permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Ascension. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

289. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Ascension would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

290. The litigation of the claims brought herein is manageable. Ascension's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

291. Adequate notice can be given to Class Members directly using information maintained in Ascension's records.

292. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

293. Further, Ascension has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief regarding the Class Members is appropriate under on a class-wide basis.

294. Likewise, issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendants breached the implied contract;

- f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and
- h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendants' wrongful conduct.

**VI. CAUSES OF ACTION**  
**COUNT I**  
**Negligence**  
**(On Behalf of Plaintiffs and the Class)**

282. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

283. Defendants require its patients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

284. Ascension gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

285. Plaintiffs and Class Members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.

286. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

287. By voluntarily undertaking and assuming the responsibility to collect and store this

data, and in fact doing so, and sharing it and using it for commercial gain, Ascension had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Ascension's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

288. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

289. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

290. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the Private Information.

291. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Ascension and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Ascension with their confidential Private Information, a necessary part of being patients at Ascension.

292. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Ascension is bound by industry standards to protect confidential Private Information.

293. Ascension was subject to an "independent duty," untethered to any contract between Ascension and Plaintiffs or the Class.

294. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

295. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

296. Ascension had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Ascension's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

297. Ascension breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;

- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- e. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations; and
- f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

298. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Ascension's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

299. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

300. Ascension's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

301. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

302. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Ascension's inadequate security

practices.

303. It was foreseeable that Ascension's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

304. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

305. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Ascension's systems or transmitted through third party systems.

306. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

307. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Ascension's possession.

308. Ascension was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

309. Ascension's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

310. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

311. But for Ascension's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

312. There is a close causal connection between Ascension's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Ascension's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

313. As a direct and proximate result of Ascension's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) damages for the unauthorized disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the lifetime cost of credit monitoring for affected individuals, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further

unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

314. Additionally, as a direct and proximate result of Ascension's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

315. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

316. Plaintiffs and Class Members are also entitled to injunctive relief requiring Ascension to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**Negligence *Per Se***  
**(On Behalf of Plaintiffs and the Class)**

317. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

318. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

319. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the

healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

320. Ascension breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

321. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

322. Plaintiffs and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiffs and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

323. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

324. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that by failing to meet its duties, Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

325. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

**COUNT III**  
**Breach Of Express Contract**  
**(On Behalf of Plaintiffs and the Class)**

326. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

327. Ascension's Notice of Privacy Practices is an agreement between Ascension and individuals who provided their PHI and PII to Ascension, including Plaintiffs and Class Members.

328. Ascension represents that its Notice of Privacy Practices applies to information it collects about individuals who seek or receive Ascension's services.

329. Ascension's Notice of Privacy Practices states that Ascension "We are committed to maintaining the privacy and confidentiality of your health information."

330. Ascension agrees to use the information for certain enumerated purposes including to: "to support our business, improve your care, educate our professionals, and evaluate provider performance," "with out business associates, who provide services for or on our behalf, such as a billing service, who help us with our business operations. All of our business associates are required to protect the privacy and security of your health information just as we do," "to notify you about possible alternative treatment options, new services, opportunities to participate in research, opportunities to provide us feedback on our services, and other health-related benefits or services," and "for Ascension fundraising purposes ...."

331. Ascension agrees to use the information for certain enumerated purposes only with written permission, including: "for marketing purposes," "for the sale of your information or for payments from third parties."

332. None of the enumerated circumstances involve sharing Plaintiffs or the Class Members' PHI with unauthorized parties.

333. Plaintiffs and Class Members on the one side and Ascension on the other formed a contract when Plaintiffs and Class Members obtained services from Ascension, or otherwise transmitted or authorized the transmission of PII and PHI to Ascension subject to its Notice of Privacy Practices.

334. Ascension breached its agreement with Plaintiffs and Class Members by failing to protect their PII and PHI. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

335. As a direct and proximate result of Ascension's breach of contract, Plaintiffs and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

**COUNT IV**  
**Breach Of Implied Contract**  
**(On Behalf of Plaintiffs and the Class)**

336. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

337. Plaintiffs and Class Members were required to deliver their Private Information to Defendants as part of the process of obtaining services from Defendants. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Ascension in exchange for services.

338. Defendants solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

339. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing medical products and/or services to Plaintiffs and Class Members.

340. Plaintiffs and the Class entrusted their Private Information to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

341. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

342. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

343. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

344. On information and belief, at all relevant times Ascension promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

345. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

346. Plaintiffs and Class Members paid money to Ascension with the reasonable belief and expectation that Ascension would use part of its earnings to obtain adequate data security. Ascension failed to do so.

347. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

348. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

349. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

350. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

351. Ascension breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised because of the Data Breach.

352. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the

systems that were exploited in the Data Breach.

353. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) damages for the unauthorized disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

354. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

355. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT V**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs and the Class)**

356. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

357. Plaintiffs brings this Count in the alternative to the breach of implied contract count

above.

358. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they paid Defendants and/or its agents for the provision of services and in so doing also provided Defendants with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

359. Ascension knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Ascension profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

360. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

361. Ascension acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

362. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information to Defendants or obtained services from Defendants.

363. Plaintiffs and Class Members have no adequate remedy at law.

364. Ascension enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident,

Ascension instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Ascension's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

365. Under the circumstances, it would be unjust for Ascension to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

366. As a direct and proximate result of Ascension's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) damages for the unauthorized disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

367. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Ascension and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Ascension from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

368. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**COUNT VI**  
**Invasion of Privacy**  
**(On Behalf of all Plaintiffs and the Class)**

369. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

370. Defendants' conduct as set forth in the foregoing paragraphs constitutes both in intrusion upon seclusion and a public disclosure of private facts.

371. Plaintiffs and the Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

372. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class, to keep their Private Information contained as a part thereof, confidential.

373. Defendant failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiffs and the Class.

374. Defendant allowed unauthorized and unknown third parties to access and examine the Private Information of Plaintiffs and the Class, by way of Defendant's failure to protect the Private Information.

375. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Class is highly offensive to a reasonable person, especially because of the highly sensitive nature of the data affected.

376. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to Defendant as part of

Plaintiffs' and the Class's relationships with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

377. Because of the intrusion, Plaintiffs' and Class Members' data was disclosed to notorious cybercriminals and other identity thieves whose mission it is to misuse PII and PHI.

378. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person and it further represents a disclosure of private facts to the public.

379. Because Plaintiffs have already begun getting alerts that their information has been published to the dark web, Plaintiffs Private Information has been published to cybercriminals and others who visit the dark web, which is no less than thousands of individuals and constitutes a substantial number such that the disclosure was public within the meaning of the tort. Additionally, the individuals to whom the disclosure was made are in a special relationship with Plaintiffs and the Class because those individuals are intent on misusing the data disclosed to them.

380. Defendant acted with a knowing and intentional state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

381. Moreover, due to the highly foreseeable nature of data breaches and the harm inherent therefrom, Defendant's failure to implement reasonable security measures was done with substantial certainty of the harm that that would and did follow.

382. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class

383. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

384. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs or Class Members.

**COUNT VII**  
**Violation of the Missouri Merchandising Practices Act,**  
**Mo. Rev. Stat. § 407.010 *et seq.***  
**(On Behalf of Plaintiffs and the Class)**

385. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

386. The Missouri Merchandising Practice Act (the “MMPA”) prohibits false, fraudulent, or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

387. The MMPA prohibits the “act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce.” Mo. Rev. Stat. § 407.020.

388. The MMPA defines “Merchandise” as “any objects, wares, goods, commodities, intangibles, real estate or services.” Mo. Rev. Stat. § 407.010(4).

389. Plaintiff, individually and on behalf of the Class, is entitled to bring an action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.20, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award the prevailing party attorneys’ fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. Mo. Rev. Stat. § 407.025.

390. Ascension is a “person” within the meaning of the MMPA in that Ascension is a domestic, not-for-profit corporation. Mo. Rev. Stat. § 407.010(5).

391. Plaintiffs and Class Members are “persons” under the MMPA because they are natural persons and they used Ascension’s services for personal, family, and/or household use.

392. The Missouri Attorney General has specified the settled meanings of certain terms used in the enforcement of the MMPA. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) Unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes, or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive, or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

393. Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., Rev. Stat. Mo. (*See Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365.

394. Pursuant to the MMPA and Mo. Code Regs. Tit. 15, § 60- 8.020, Ascension's acts and omissions fall within the meaning of "unfair."

395. Defendants engaged in a "trade" or "commerce" within the meaning of the MMPA with regard to services which are supposed to keep Plaintiff's and the Class Members's Private Information safe and secure.

396. Ascension engaged in unlawful practices and deceptive conduct, which emanated from its Missouri headquarters, in violation of the MMPA by omitting and/or concealing material facts related to the safety and security of Plaintiff's and the Class Members's Private Information. Ascension's unfair and unethical conduct of failing to secure Private Information and failing to disclose the Data Breach caused substantial injury to consumers in that the type of consumers' personal information impacted by the breach can be used to orchestrate a host of fraudulent activities, including medical, insurance, and financial fraud and identity theft. The impacted consumers have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

397. Defendants' conduct of failing to secure data required Plaintiffs and the Class to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Private Information.

398. Defendants' conduct of concealing, suppressing, or otherwise omitting material facts regarding the Data Breach was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

399. By failing to secure sensitive data and failing to disclose and inform Plaintiffs and Class Members about the Breach of Private Information, Defendants engaged in acts and practices that constitute unlawful practices in violation of the MMPA. Mo. Ann. Stat. §§ 407.010, *et seq.*

400. Defendants engaged in unlawful practices and deceptive conduct in the course of their business that violated the MMPA including misrepresentations and omissions related to the safety and security of Plaintiff's and the Class's Private Information. Mo. Rev. Stat. § 407.020.1.

401. As a direct and proximate result of these unfair and deceptive practices, Plaintiffs and each Class member suffered actual harm in the form of money and/or property because the disclosure of their Private Information has value encompassing financial data and tangible money.

402. Defendants' "unfair" acts and practices include:

- a. by utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;
- b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;
- c. failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

- d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and
- e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

403. Defendants' unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures; and
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members'

personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

404. Defendants' misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of medical products and/or services.

405. Defendants' deceptive practices misled Plaintiffs and the Class and would cause a reasonable person to enter into transactions with Defendants that resulted in damages.

406. As such, Plaintiffs and the Class seek: (1) to recover actual damages sustained; (2) to recover punitive damages; (3) to recover reasonable attorneys' fees and costs; and (4) such equity relief as the Court deems necessary or proper to protect Plaintiffs and the members of the Class from Ascension's deceptive conduct and any other statutorily available damages or relief the court deems proper.

#### **COUNT VIII**

#### **Violation of the Arkansas Deceptive Trade Practices Act, A.C.A. §§ 4-88-101, *et seq.* (On Behalf of Plaintiff Dunn and the Arkansas Subclass)**

407. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

408. Alternatively, or in addition, Plaintiff Dunn and the Arkansas Subclass members bring this claim for violation of Arkansas's Deceptive Trade Practices Act, A.C.A. §§ 4-88-101, *et seq.*

409. Ascension is a "person" as defined by A.C.A. § 4-88-102(5).

410. Ascension's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

411. Ascension advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

412. The Arkansas Deceptive Trade Practices Act (“ADTPA”), A.C.A. §§ 4-88-101, et seq., prohibits unfair, deceptive, false, and unconscionable trade practices.

413. Ascension engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;
- b. Advertising goods or services with the intent not to sell them as advertised;
- c. Employing consistent bait-and-switch advertising of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced by acts demonstrating an intent not to sell the advertised product or services;
- d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and
- e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

414. Ascension’s unconscionable, false, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Dunn's and Arkansas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Dunn's and Arkansas Subclass members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110- 104(b).

415. Ascension's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Ascension's data security and ability to protect the confidentiality of consumers' Private Information.

416. Ascension intended to mislead Plaintiff Dunn and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

417. Had Ascension disclosed to Plaintiff Dunn and Arkansas Subclass members that its data systems were not secure and, thus, vulnerable to attack, Ascension would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Ascension accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Plaintiff Dunn and the Arkansas Subclass members acted reasonably in relying on Ascension's misrepresentations and omissions, the truth of which they could not have discovered.

418. Ascension acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Dunn's and Arkansas Subclass

members' rights.

419. As a direct and proximate result of Ascension's unconscionable, unfair, and deceptive acts or practices and Plaintiff Dunn's and Arkansas Subclass members' reliance thereon, Plaintiff Dunn and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

420. Plaintiff Dunn and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT IX**  
**Violation of the Florida Deceptive and Unfair Trade Practices Act,**  
**Fla. Stat. §§ 501.201, *et seq.***  
**(On Behalf of Plaintiff Brown and the Florida Subclass)**

421. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

422. Alternatively, or in addition, Plaintiff Brown and Florida Subclass members bring this claim for violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*

423. At all times relevant herein, Plaintiff Brown and the Florida Subclass members are "consumers" as defined under Fla. Stat. § 501.203(7).

424. Ascension, while operating its healthcare facilities in Florida, engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the conduct of "trade or commerce" (as defined in the Florida

Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.203), in violation of Fla. Stat. § 501.203, including the following:

- a. Ascension misrepresented and fraudulently advertised material facts to Plaintiff Brown and the Florida Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Brown's and the Florida Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft;
- b. Ascension misrepresented and fraudulently advertised material facts to Plaintiff Brown and the Florida Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Brown's and the Florida Subclass members' Private Information;
- c. Ascension omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff Brown's and the Florida Subclass members' Private Information;
- d. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff Brown's and the Florida Subclass members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and Fla. Stat. § 501.171.

- e. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff Brown and Florida Subclass members in a timely and accurate manner, contrary to the duties imposed by Fla. Stat. § 501.171;
- f. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Brown's and the Florida Subclass members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

425. As a direct and proximate result of Ascension's deceptive trade practices, Plaintiff Brown and Florida Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the payment for purchases they otherwise would not have made or overpayment for the purchases they did make and the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

426. The above unfair and deceptive practices and acts by Ascension were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

427. Ascension knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff Brown's and the Florida Subclass members' Private Information and that risk of a data breach or theft was highly likely. Ascension's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Brown and

the Florida Subclass.

428. Florida Class Members seek relief under Fla. Stat. § 501.201 et seq., including damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs pursuant to Fla. Stat. § 501.2105.

**COUNT X**  
**Violation of the Illinois Personal Information Protection Act,**  
**815 Ill. Comp. Stat. Ann. § 530/1, et seq.**  
**(On Behalf of Plaintiffs Boyden, Negron, and the Illinois Subclass)**

429. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

430. Alternatively, or in addition, Plaintiffs Boyden, Negron, and Illinois Subclass members bring this claim for violation of Illinois's statute on the Protection of Personal Information.

431. Ascension is a data collector that owns or licenses or maintains or stores computerized data that includes Personal Information as defined by 815 Ill. Comp. Stat. Ann. § 530/5.

432. Plaintiffs Boyden, Negron, and Illinois Subclass members' Private Information (e.g., Social Security numbers) includes "Personal Information" as covered under 815 Ill. Comp. Stat. Ann. § 530/5(1)-(2).

433. Ascension is required to accurately notify Plaintiff Boyden and Illinois Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiffs Boyden, Negron, and Illinois Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under 815 Ill. Comp. Stat. Ann. § 530/10(a).

434. Because Ascension was aware of a breach of its security system that was reasonably

likely to have caused misuse of Plaintiffs Boyden, Negron, and Illinois Subclass members' Personal Information, Ascension had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 815 Ill. Comp. Stat. Ann. § 530/10(a). By failing to disclose the Data Breach in a timely and accurate manner, Ascension violated 815 Ill. Comp. Stat. Ann. § 530/10(a).

435. As a direct and proximate result of Ascension's violations of 815 Ill. Comp. Stat. Ann. § 530/10(a), Plaintiffs Boyden, Negron, and Illinois Subclass members suffered damages, as described above.

436. Plaintiffs Boyden, Negron, and Illinois Subclass members seek relief under 815 Ill. Comp. Stat. Ann. § 530/10(a), including equitable relief.

#### **COUNT XI**

##### **Violation of Illinois Consumer Fraud and Deceptive Business Practices Act.**

##### **815 Ill. Comp. Stat. Ann. § 505/1, *et seq.***

##### **(On Behalf of Plaintiffs Boyden, Negron, and the Illinois Subclass)**

437. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

438. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") prohibits false, fraudulent, or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

439. The ICFA prohibits "unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact . . . in the conduct of any trade or commerce" including "whether any person has in fact been misled, deceived or damaged thereby." 815 Ill. Comp. Stat. Ann. § 505/2.

440. The ICFA defines “Merchandise” as including “any objects, wares, goods, commodities, intangibles, real estate situated outside the State of Illinois, or services.” 815 Ill. Comp. Stat. Ann. § 505/1(b).

441. Plaintiffs, individually and on behalf of the Illinois Subclass, is entitled to bring to bring this action pursuant to 815 Ill. Comp. Stat. Ann. § 505/10(a), which provides in relevant part that “any person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person. The court, in its discretion may award actual economic damages or any other relief which the court deems proper[.]” Moreover, “except as provided in subsections (f), (g), and (h) of this Section, in any action brought by a person under this Section, the Court may grant injunctive relief where appropriate and may award, in addition to the relief provided in this Section, reasonable attorney's fees and costs to the prevailing party.” 815 Ill. Comp. Stat. Ann. § 505/10(a)(c).

442. Plaintiffs Boyden, Negron, and Illinois Subclass members are “consumers” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(e).

443. The acts and practices described herein are “trade,” and “commerce” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(f).

444. Ascension is a “person” as defined by 815 Ill. Comp. Stat. Ann. § 505/1(c).

445. Ascension advertised, offered, or sold goods or services in Illinois and engaged in trade or commerce directly or indirectly affecting the people of Illinois.

446. Ascension engaged in deceptive and unfair acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Boyden, Negron, and Illinois Subclass members’ Private Information, which was a direct and proximate cause of

the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Boyden, Negron, and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. Ann. § 530/1 et seq., which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs Boyden, Negron, and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Boyden, Negron, and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. Ann. § 530/1 et seq.;
- f. Omitting, suppressing, and concealing the material fact that it did not

reasonably or adequately secure Plaintiffs Boyden, Negron, and Illinois Subclass members' Private Information; and

- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Boyden, Negron, and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. Ann. § 530/1 et seq.

447. Ascension's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Ascension's data security and ability to protect the confidentiality of consumers' Private Information.

448. Ascension intended to mislead Plaintiffs Boyden, Negron, and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

449. Had Ascension disclosed to Plaintiffs Boyden, Negron, and Illinois Subclass members that its data systems were not secure and, thus, vulnerable to attack, Ascension would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Ascension accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Plaintiffs Boyden, Negron, and Illinois Subclass members acted reasonably in relying on Ascension's misrepresentations and omissions, the truth of which they could not have discovered.

450. As a direct and proximate result of Ascension's unfair and deceptive acts or practices and Plaintiffs Boyden, Negron, and Illinois Subclass members' reliance thereon,

Plaintiffs Boyden, Negron, and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

451. Plaintiffs Boyden, Negron, and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT XII**  
**Violation of the Oklahoma Consumer Protection Act,**  
**Okla. Stat. Ann. tit. 15, § 751, *et seq.***  
**(On Behalf of Plaintiff Hayes and the Oklahoma Subclass)**

452. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

453. Alternatively, or in addition, Plaintiffs Hayes and Oklahoma Subclass members bring this claim for violation of the Oklahoma Consumer Protection Act.

454. The purchases of healthcare services and medical supplies from Ascension by Plaintiffs Hayes and the members of the Oklahoma Subclass constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752.

455. Ascension engaged in unlawful, unfair, and deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale of healthcare services and medical supplies to Plaintiffs Hayes and the Oklahoma Subclass members in violation of Okla. Stat. tit. 15, § 753, including the following:

- a. Ascension knowingly, or with reason to know, misrepresented material facts pertaining to the sale of medical services and supplies to Plaintiffs

Hayes and the Oklahoma Subclass members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs Hayes' and the Oklahoma Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft in violation of Okla. Stat. tit. 15, § 753(5) and (8);

- b. Ascension knowingly, or with reason to know, misrepresented material facts pertaining to the sale of medical supplies and services to Plaintiffs Hayes and the Oklahoma Subclass members by representing that Ascension did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs Hayes' and the Oklahoma Subclass members' Private Information in violation of Okla. Stat. tit. 15, § 753(5) and (8);
- c. Ascension omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiffs Hayes' and the Oklahoma Subclass members' Private Information in violation of Okla. Stat. tit. 15, § 753(5) and (8);
- d. Ascension engaged in unfair, unlawful, and deceptive trade practices with respect to the sale of medical services and supplies by failing to maintain the privacy and security Plaintiffs Hayes' and the Oklahoma Subclass members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Okla. Admin. Code

§§ 365:35-1-40, 365:35-1-20;

- e. Ascension engaged in unlawful, unfair, and deceptive trade practices with respect to the sale of medical services and supplies by failing to disclose the Data Breach to Plaintiffs Hayes and the Oklahoma Subclass members in a timely and accurate manner, in violation of 24 Okla. Sta. Ann. § 163(A);
- f. Ascension engaged in unlawful, unfair, and deceptive trade practices with respect to the sale of medical supplies and services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs Hayes' and the Oklahoma Subclass members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

456. The above unlawful, unfair, and deceptive trade practices and acts by Ascension were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

457. As a direct and proximate result of Ascension's deceptive acts and practices, Plaintiffs Hayes and Oklahoma Subclass members suffered injury and/or damages.

458. Plaintiffs Hayes and Oklahoma Subclass members seek relief under Okla. Stat. Ann. tit. 15, § 761.1 including injunctive relief, actual damages, and attorneys' fees and costs.

### **COUNT XIII**

#### **Breach of Confidentiality of Health Records, Wis. Stat. § 146.81, *et seq.* (On Behalf of Plaintiffs Farrand, Radley, and the Wisconsin Subclass)**

459. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

460. Alternatively, or in addition, Plaintiffs Farrand, Radley, and Wisconsin Subclass

members bring this claim for Breach of Confidentiality of Patient Health Records, pursuant to Wis. Stat. §§ 146.81, et seq., which states: “All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient.” Wis. Stat. § 146.82(1).

461. The stolen Private Information belonging to Plaintiffs Farrand, Radley, and the Wisconsin Subclass are “Health care records” under Wis. Stat. § 146.81(4).

462. Ascension violated Wis. Stat. §§ 146.81, et seq. when it compromised, allowed access to, released, and disclosed patient health care records and PHI to third parties without the informed consent or authorization of Plaintiffs Farrand, Radley, and the members of the Wisconsin Subclass. Ascension did not and does not have express or implied consent to disclose, allow access to, or release Plaintiffs Farrand, Radley’s, and Wisconsin Subclass members’ Private Information. To the contrary, Ascension expressly undertook a duty and obligation to Plaintiffs Farrand, Radley, and the members of the Wisconsin Subclass when it told them their Private Information would be private and secure.

463. Ascension did not disclose to or warn Plaintiffs Farrand, Radley, and Wisconsin Subclass members that their Private Information could be compromised, stolen, released, or disclosed to third parties without their consent as a result of Ascension’s computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiffs Farrand, Radley, and Wisconsin Subclass members did not know or expect, or have any reason to know or suspect, that Ascension’s computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their Private Information to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to Plaintiffs Farrand,

Radley, and Wisconsin Subclass members, and on Ascension's website.

464. Wis. Stat. § 146.84(1)(b) states

Any person, including the state or any political subdivision of the state, who violates Wis. Stat. s. 146.82 or 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than \$25,000 and costs and reasonable actual attorney fees.

465. Wis. Stat. § 146.84(1)(bm) states,

Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. s. 146.82 or 146.83 shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than \$1,000 and costs and reasonable actual attorney fees.” Wis. Stat. § 146.84(1)(bm).

466. Wis. Stat. § 146.84(1)(c) states,

An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection.

467. Actual damages are not a prerequisite to liability for statutory or exemplary damages under Wis. Stat. § 146.81. A simple comparison of other Wisconsin statutes (e.g., Wis. Stat. § 134.97(3)(a) and (b), “Civil Liability; Disposal And Use” of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. § 146.84 when it explicitly did so in other privacy statutes. See Wis. Stat. § 134.97(3)(a) and (b).

468. Similarly, the Wisconsin Legislature made it clear that the exemplary damages referred to in Wis. Stat. § 146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statute (Wis. Stat. § 895.043(2), “Scope” of punitive damages), specifically and unequivocally excludes an award of “exemplary damages” under Wis. Stat. §§ 146.84(1)(b) and (bm) from the scope of “punitive damages” available under Section 895.043.19. In short,

exemplary damages under Wis. Stat. § 146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been “injured” as a result of a negligent data breach like the one at issue here.

469. Plaintiffs Farrand, Radley, and Wisconsin Subclass members request that the Court issue declaratory relief declaring Ascension’s practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PHI data between Ascension and third parties unlawful. Plaintiffs Farrand, Radley, and Wisconsin Subclass members further request the Court enter an injunction requiring Ascension to cease the unlawful practices described herein, and enjoining Ascension from disclosing or using PHI without first adequately securing or encrypting it.

470. Plaintiffs Farrand, Radley, and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by Wis. Stat. § 146.84(1)(bm), including injunctive relief and attorneys’ fees.

**COUNT XIV**  
**Violation of Wisconsin Deceptive Trade Practices Act,**  
**Wis. Stat. §§ 100.18, *et seq.***  
**(On Behalf of Plaintiffs Farrand, Radley, and the Wisconsin Subclass)**

471. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

472. Alternatively, or in addition, Plaintiffs allege that Ascension’s conduct violates Wisconsin’s Deceptive Trade Practices Act, Wis. Stat. § 100.18 (the “WDTPA”), which provides that:

[no] firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which

is untrue, deceptive or misleading.

473. Plaintiffs Farrand, Radley, and Wisconsin Subclass members “suffer[ed] pecuniary loss because of a violation” of the WDTA. Wis. Stat. § 100.18(11)(b)(2).

474. Ascension violated the WDTA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breach, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breach, so as to safeguard Private Information from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; and (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breach, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access.

475. The purpose of Ascension’s misrepresentations set forth herein was to ensure that Plaintiffs Farrand, Radley, and Wisconsin Subclass members would entrust Ascension with their data, thereby increasing the sales and use of Ascension’s goods and services.

476. Ascension knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breach and theft was high. Ascension’s actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs Farrand, Radley, and Wisconsin Subclass members.

477. Plaintiffs Farrand, Radley, and Wisconsin Subclass members relied upon Ascension's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

**COUNT XV**

**Violation of Notice of Unauthorized Acquisition of Personal Information,**

**Wis. Stat. §§ 134.98(2), *et seq.***

**(On Behalf of Plaintiffs Farrand, Radley, and the Wisconsin Subclass)**

478. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

479. Alternatively, or in addition, Plaintiffs Farrand, Radley, and the Wisconsin Subclass allege that Ascension's conduct violates Wisconsin's statute regarding Notice of Unauthorized Acquisition of Personal Information, Wis. Stat. §§ 134.98(2), *et seq.*

480. Ascension is a business that maintains or licenses "Personal Information" Plaintiffs Farrand, Radley's, and Wisconsin Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

481. Ascension is required to accurately notify Plaintiffs Farrand, Radley, and Wisconsin Subclass members if it knows that Personal Information in its possession has been acquired by a person whom it has not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

482. Because Ascension knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Ascension had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

483. By failing to disclose the Ascension data breach in a timely and accurate manner,

Ascension violated Wis. Stat. § 134.98(2).

484. As a direct and proximate result of Ascension's violations of Wis. Stat. § 134.98(3)(a), Plaintiffs Farrand, Radley, and Wisconsin Subclass members suffered damages, as described above.

485. Plaintiffs Farrand, Radley, and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief, as defined by Wis. Stat. § 134.98(2).

**COUNT XVI**

**Michigan Identity Theft Protection Act,  
Mich. Comp. Laws Ann. § 445.72, *et seq.*  
(On Behalf of Plaintiff Willis and the Michigan Subclass)**

486. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

487. Plaintiff Willis bring this claim on behalf of themselves and the Michigan Sub-Class.

488. Ascension is a business that owns or licenses computerized data that includes "Personal Information" (for the purpose of this count, "Private Information") within the meaning of Mich. Comp. Laws Ann. § 445.72(1).

489. Plaintiffs Willis and Sub-Class Members' PII and PHI includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

490. Ascension is required to accurately notify Plaintiffs Willis and Sub-Class Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

491. Ascension was required to provide written notice in a "clear and conspicuous manner." Mich. Comp. Laws Ann. § 445.72(6). Because Ascension discovered a security breach

and had notice of a security breach (where Private Information was accessed or acquired by unauthorized persons), Ascension had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

492. By failing to disclose the Data Breach in a timely and accurate manner and provide clear and conspicuous notice, Ascension violated Mich. Comp. Laws Ann. § 445.72(4).

493. As a direct and proximate result of Ascension's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiffs and Sub-Class Members suffered damages, and will continue to suffer damages, as described above.

494. Plaintiffs Willis and Sub-Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

**COUNT XVII**  
**Michigan Consumer Protection Act,**  
**Mich. Comp. Laws Ann. § 445.903, *et seq.***  
**(On Behalf of Plaintiff Willis and the Michigan Subclass)**

495. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

496. Plaintiffs and Willis bring this claim on behalf of the Michigan Sub-Class.

497. Defendants and Michigan Sub-Class are "persons" under Mich. Comp. Laws Ann. § 445.902(d).

498. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

499. Defendants engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing their goods and services to have characteristics, uses and

benefits which they did not have, violating Mich. Comp. Laws Ann. § 445.903(1)(c).

- b. Making a representation material to Plaintiffs and Sub-Class's transaction such that one reasonably believes the represented state of Ascension's affairs to be something which it is not, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb).
- c. Failing to reveal facts material to Plaintiffs and Sub-Class's transaction in light of representations of fact made in a positive manner, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).
- d. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Sub-Class Members' Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Sub-Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and other laws, which was a direct and proximate cause of the Data Breach;
- g. Failing to ensure that it could access and maintain Class Members' Private Information on its systems and thus continue to provide treatment to them;

Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Sub-Class Members' Private Information, including by implementing and maintaining reasonable security measures;

- h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Sub-Class Members' PII, including duties imposed by the and the FTC Act, 15 U.S.C. § 45, HIPAA, and other laws;
- i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Sub-Class Members' Private Information;
- j. Failing to timely notify Plaintiffs and Sub-Class Members of the Data Breach violation under the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. § 445.72(1).

500. Ascension's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Ascension's data security and ability to protect the confidentiality of consumers' Private Information.

501. Ascension intended to mislead Plaintiffs and Sub-Class Members and induce them to rely on its misrepresentations and omissions.

502. Had Ascension disclosed to Plaintiffs and Class Members that its systems were not secure and, thus, vulnerable to attack, Ascension would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Ascension was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiff, Class Members, and Sub-Class Members.

Ascension accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Ascension held itself out as maintaining a secure platform for Private Information data, Plaintiff, Class Members, and Sub-Class Members acted reasonably in relying on Ascension's misrepresentations and omissions, the truth of which they could not have discovered.

503. Ascension acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiffs and Sub-Class Members' rights.

504. As a direct and proximate result of Ascension's unfair and deceptive acts and practices, Plaintiffs and Sub-Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; and delayed medical care and treatment, costs associated with finding alternate healthcare providers and treatments, and unnecessary pain and suffering, and emotional distress.

505. Plaintiffs and Sub-Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages, restitution, injunctive relief, and any other relief that is just and proper.

**COUNT XVIII**  
**Violation of the Indiana Deceptive Consumer Sales Act**  
**Ind. Code §§ 24-5-0.5-0.1, *et seq.***  
**(On Behalf of Plaintiffs Gounaris, Pitchers, and the Indiana Subclass)**

506. Plaintiffs re-allege and incorporate by reference the allegations in paragraph 1 through 281, as if fully set forth herein.

507. Alternatively, or in addition, Plaintiffs Pitchers, Gounaris and Indiana Subclass

members bring this claim for violation of Indiana's Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3(a) (“IDCSA”), which prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

508. Ascension is a “supplier” of consumer services as provided by Ind. Code § 24-5-0.5-2. Plaintiffs Pitchers, Gounaris and Indiana Subclass members are “consumers” of Ascension's services.

509. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of “consumer transactions,” in violation of the IDCSA. As a regular part of its business, Ascension operates health care facilities in Indiana. It accepts payments from customers, like Plaintiffs Pitchers, Gounaris and the Indiana Subclass members, for Ascension services and medical supplies. On information and belief, consumer transactions were processed in Indiana and health care services were performed in Indiana.

510. In connection with its consumer transactions, Ascension engaged in unfair, abusive or deceptive acts, omissions or practices by, inter alia, engaging in the following conduct:

- a. failing to maintain sufficient security to keep Plaintiffs Pitchers, Gounaris’s and the Indiana Subclass members’ Private Information from being hacked and stolen;
- b. misrepresenting material facts to Plaintiffs Pitchers, Gounaris and the Indiana Subclass members, in connection with providing health care services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs Pitchers, Gounaris’s and the Indiana Subclass members’ Private Information as contained in its Notice of Privacy Practices;

- c. misrepresenting material facts to Plaintiffs Pitchers, Gounaris and the Indiana Subclass members, in connection with providing health care services, by representing that Ascension did and would comply with the requirements of relevant federal and state law pertaining to the privacy and security of Plaintiffs Pitchers, Gounaris's and the Indiana Subclass members' Private Information, such requirements included, but are not limited to, those imposed by laws such as the Federal Trade Commission Act (15 U.S.C. § 45) and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and
- d. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs Pitchers, Gounaris's and the Indiana Subclass members' Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

511. Ascension knew that its computer systems and data security practices were inadequate to safeguard Plaintiffs Pitchers, Gounaris's and the Indiana Subclass members' Private Information and that risk of a data breach or theft was highly likely. Nevertheless, it did nothing to warn Plaintiffs Pitchers, Gounaris and the Indiana Subclass members about its data insecurities, and instead affirmatively promised that it would maintain adequate security. This was a deliberate effort to mislead consumers, such as Plaintiffs Pitchers, Gounaris and the Indiana Subclass members, in order to encourage them to receive health care services even while Ascension knew that its consumers' sensitive Private Information was vulnerable.

512. The above unfair and deceptive practices and acts or omissions by Ascension were

done as a part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

513. As a direct and proximate result of Ascension's deceptive trade practices, Plaintiffs Pitchers, Gounaris and the Indiana Subclass members suffered damages and injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

514. As a direct and proximate result of Ascension's deceptive trade practices, Plaintiffs Pitchers, Gounaris and the Indiana Subclass members are now likely to suffer identity theft crimes and face a lifetime risk of identity theft crimes.

515. Plaintiffs Pitchers, Gounaris and the Indiana Subclass members seek relief under Ind. Code § 24-5-0.5-4, including damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

516. Plaintiffs Pitchers, Gounaris and the Indiana Subclass members injured by Ascension's unfair and deceptive trade practices also seek treble damages pursuant to Ind. Code § 24-5-0.5-4(i).

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

- A.** For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;
- B.** For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
- a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
  - b. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - c. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
  - d. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class Members' respective lifetimes;
  - e. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;
  - f. prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;
  - g. requiring Defendants to engage independent third-party security

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

- h. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- i. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;
- j. requiring Defendants to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers cannot gain access to portions of Defendants' systems;
- k. requiring Defendants to conduct regular database scanning and securing checks;
- l. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- m. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel

how to identify and contain a breach when it occurs and what to do in response to a breach;

- n. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
- o. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- p. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect herself;
- q. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and
- r. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final

judgment;

- D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs hereby demand a trial by jury on all claims so triable.

Date: October 7, 2024

Respectfully Submitted,

/s/Norman E. Siegel

Norman E. Siegel #44378 (MO)  
Tanner J. Edwards #68039 (MO)  
**STUEVE SIEGEL HANSON LLP**  
460 Nichols Road, Suite 200  
Kansas City, Missouri 64112  
Telephone: 816-714-7100  
siegel@stuevesiegel.com  
tanner@stuevesiegel.com

John F. Garvey #35879 (MO)  
Colleen Garvey #72809 (MO)  
Ellen A. Thomas, #73043 (MO)  
**STRANCH JENNINGS & GARVEY, PLLC**  
701 Market Street, Suite 1510  
St. Louis, Missouri 63101  
Telephone: (314) 390-6750  
jgarvey@stranchlaw.com  
cgarvey@stranchlaw.com  
ethomas@stranchlaw.com

J. Gerard Stranch, IV # 23045 (TN)  
**STRANCH JENNINGS & GARVEY, PLLC**  
223 Rosa L. Parks Avenue, Suite 200  
Nashville, Tennessee 37203  
Telephone: (615) 254-8801

gstranch@stranchlaw.com

**Interim Co-Lead Counsel**

Gary M. Klinger (*Pro Hac Vice*)  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN PLLC**  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60606  
Telephone: (866) 252-0878  
gklinger@milberg.com

Jeff Ostrow (*Pro Hac Vice* forthcoming)  
**KOPELOWITZ OSTROW P.A.**  
One West Las Olas Blvd., Suite 500  
Fort Lauderdale, FL 33301  
Telephone: (954) 332.4200  
ostrow@kolawyers.com

David M. Berger (*Pro Hac Vice*)  
**GIBBS LAW GROUP LLP**  
1111 Broadway, Suite 2100  
Oakland, CA 94607  
Telephone: (510) 350-9700  
dmb@classlawgroup.com

Maureen Brady, #57800 (MO)  
**MCSHANE & BRADY, LLC**  
4006 Central Street  
Kansas City, MO 64111  
Telephone: (816) 888-8010  
mbrady@mcshanebradylaw.com

Don Downing, #30405 (MO)  
**GRAY RITTER GRAHAM PC**  
701 Market Street, Suite 800  
St. Louis, MO 63101  
Telephone: (314) 241-5620  
ddowning@grgpc.com

Laurence D. King (*Pro Hac Vice*)  
**KAPLAN FOX**  
1999 Harrison Street, Suite 1560  
Oakland, CA 94612  
Telephone: (415) 772-4700  
lking@kaplanfox.com

Sabita Soneji  
**TYCKO & ZAVAREEI LLP**  
1970 Broadway, Suite 1070  
Oakland, CA 94612  
Telephone: (510) 254-6808  
ssoneji@tzlegal.com

Lynn Toops (Pro Hac Vice filed)  
**COHEN & MALAD LLP**  
One Indiana Square, Suite 1400  
Indianapolis, IN 46204  
Telephone: (317) 636-6481  
ltoops@cohenandmalad.com

Tiffany Yiatriis, #58197 (MO)  
**CONSUMER PROTECTION LEGAL, LLC**  
308 Hutchinson Road  
Ellisville, MO 63011  
Telephone: (314) 541-0317  
tiffany@consumerprotectionlegal.com

*Attorneys for Plaintiffs and the Proposed Class*